Propostas de Pesquisa de Segurança em Redes Sem Fio

André Peres[1], Raul Fernando Weber[2]
[1]Faculdade de Informática – Universidade Luterana do Brasil (ULBRA)
92420-280 – Canoas RS – Brasil
[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brasil
{peres,weber} peres@ulbra.tche.br, weber@inf.ufrgs.br

Resumo. *Este artigo descreve uma proposta de modelos para pesquisa sobre os aspectos de segurança em redes sem fio padrão IEEE 802.11. São apresentadas as características de funcionamento deste tipo de rede consideradas relevantes para a segurança, o modo de funcionamento do protocolo de segurança WEP (Wired Equivalent Privacy), alguns problemas relacionados a este protocolo levantados por outros estudos, e possíveis modelos de estudo para melhorias na segurança desse tipo de rede.*

1. Introdução

As redes de computadores locais sem fio padrão IEEE 802.11[1] estão se tornando uma realidade para um grande conjunto de instituições e empresas. Estas redes permitem uma série de novas funcionalidades para troca de informações, tais como a facilidade de mobilidade de dispositivos, portabilidade e flexibilidade de conexões. As novas tecnologias de redes prometem o aumento da produtividade com custos relativamente baixos.

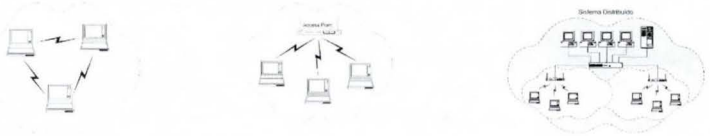
A forma de conexão e de compartilhamento é estabelecida de acordo com a arquitetura adotada, sendo definidas as arquiteturas de redes *ad hoc*; redes de infra-estrutura básica e; redes de infra-estrutura.

As redes *ad hoc* são compostas por estações independentes, sendo criadas de maneira espontânea por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência. São denominadas redes IBSS (*Independent Basic Service Set*). Um exemplo de rede *ad hoc* está representado na figura 1a.

As redes de infra-estrutura básica são formadas por um conjunto de estações sem fio, controladas por um dispositivo coordenador denominado *Access Point* (AP). Todas as mensagens são enviadas ao AP que as repassa aos destinatários. Estas redes são denominadas BSS (*Basic Service Set*) e um exemplo deste tipo de rede é apresentado na figura 1b.

As redes de infra-estrutura são também denominadas ESS (*Extended Service Set*). Estas redes são a união de diversas redes BSS conectadas através de outra rede com ou sem fio. A estrutura deste tipo de rede é composta por um conjunto de APs interconectados, permitindo que um dispositivo migre entre dois pontos de acesso da rede. As estações vêem a rede como um elemento único. Um exemplo de rede ESS é apresentado na figura 1c.

A utilização de conexões sem fio implica na ausência de limites físicos definidos com precisão, já que a abrangência dos dispositivos é de difícil definição e na falta de controle da propagação de informações e de acesso físico.



a b c

Figura 1 – redes *ad hoc* (a); BSS (b) e ESS (c)

Qualquer equipamento que possui acesso à área de abrangência da rede possui acesso aos dados sendo transmitidos. Isto significa que, para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos para o controle de autenticação e confidencialidade.

É importante salientar que a segurança que deve ser adicionada encontra-se no nível de enlace de dados. Isto se deve ao fato de que os aplicativos e protocolos de níveis superiores foram desenvolvidos contando com a segurança física disponível nas redes com fios. O nível de enlace das redes sem fio deve, então, prover características de segurança que compatibilizem estes dois tipos de conexão, e possibilitem a execução de aplicativos sem riscos.

A segurança no nível de enlace que deveria garantir a compatibilidade entre conexões com e sem fios foi prevista no padrão IEEE 802.11 através do protocolo WEP (*Wired Equivalent Privacy*). Este protocolo provou-se ineficiente em uma série de estudos [2] [3] e atualmente encontra-se em fase de reformulação por um grupo especial da IEEE, o grupo IEEE 802.11i. Os mecanismos de segurança previstos pelo padrão são a autenticação de dispositivos e a confidencialidade de dados.

2. Protocolo de segurança do IEEE 802.11 – WEP

O protocolo de segurança WEP tem por objetivo tornar a rede sem fios tão segura quanto uma rede com fios. Para realizar suas funções, o protocolo WEP possui os seguintes mecanismos:

- um segredo comum compartilhado entre as estações envolvidas;
- um algoritmo de criptografia baseado no RC4, utilizado para gerar o fluxo de dados cifrado.

O protocolo WEP funciona utilizando o gerador de números pseudo-aleatórios PRNG (*Pseudo-Random Number Generator*), do RC4. A semente para geração da chave é uma combinação do segredo compartilhado entre as estações com um vetor aleatório de 24 bits chamado IV (*Initialization Vector*).

A chave gerada pelo PRNG utilizando o segredo compartilhado concatenado com o IV como semente é utilizada em operações xor com a mensagem original, produzindo o texto cifrado [4].

Devido à grande taxa de perda de quadros de enlace, é inviável a utilização de uma chave única de sessão entre transmissor e receptor. A necessidade de sincronismo de chaves faz com que cada quadro de enlace utilize uma chave de criptografia diferente.

Para cada quadro, o protocolo WEP deve selecionar um IV diferente, permitindo que o segredo compartilhado permaneça o mesmo, mas a semente se altere [5].

Como o destinatário da mensagem deve criar a chave de decifragem a partir da mesma semente, o remetente envia o IV escolhido sem criptografia junto com o quadro. Desta forma, o destinatário pode unir o segredo compartilhado com o IV escolhido e utilizar estas informações como semente no PRNG.

Para verificar que os dados não foram alterados durante a comunicação, é utilizado um algoritmo redundante do tipo CRC-32 (*Cyclic Redundancy Check*) denominado ICV - *Integrity Check Value*.

A figura 2a apresenta o esquema de cifragem de mensagens do protocolo WEP, enquanto a figura 2b apresenta a decifragem.

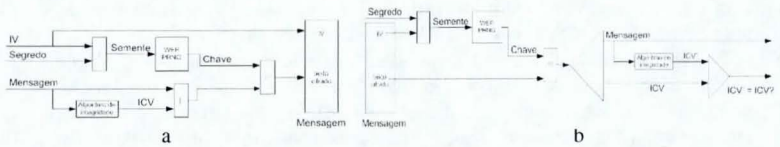


Figura 2 – WEP

2.1 Possíveis ataques ao protocolo WEP

Para obter acesso a uma rede sem fios, todas as estações devem ser autenticadas com o AP. Para realizar a autenticação, o padrão IEEE 802.11 especifica a autenticação *OpenSystem*, ou autenticação nula, na qual o AP aceita qualquer estação (esta é a autenticação padrão); ou autenticação *Shared Key* que implementa o WEP para autenticar as estações e trocar informações.

A autenticação *shared key* é implementada através da escolha de um texto desafio pelo AP que o repassa ao requisitante (cliente). O cliente deve cifrar este texto utilizando o segredo compartilhado e devolver o resultado ao AP. O AP pode agora verificar se o cliente possui o segredo compartilhado e o autenticar.

Em ambos modelos é possível realizar ataques na rede, porém, no restante deste trabalho serão consideradas as redes que implementam autenticação *Shared Key*.

A utilização de diferentes IVs não impede a repetição de chaves, pois o seu pequeno tamanho (24 bits) acarreta em repetições. Por exemplo, em uma rede onde o AP envia quadros de 1500 bytes a 11 Mbps ocorrerão repetições a cada: (1500*8)*(2^24)/(11*10^6) aproximadamente 18000 segundos, ou seja, a cada 5 horas.

O algoritmo RC4 ao ser utilizado nas redes sem fio, devido à repetição de IVs, apresenta fraquezas. O trabalho [6] apresenta os resultados de uma pesquisa sobre fraquezas do algoritmo RC4 utilizado nas redes sem fio. Estas fraquezas dizem respeito a um grande número de chaves fracas geradas pelo RC4, e pela possibilidade de descobrir bits do

segredo compartilhado a partir da análise/conhecimento dos primeiros bits da mensagem cifrada. Os primeiros bits são sempre conhecidos pelo atacante devido ao cabeçalho LLC (*Logical Link Control*), o qual inclui sempre a mesma informação (0xaa) no início do texto a ser cifrado. A partir dos resultados obtidos neste trabalho foram desenvolvidos programas como o AirSnort [7], o qual consegue obter o segredo compartilhado entre as estações através da análise do tráfego da rede. Ao obter o segredo compartilhado, a privacidade da rede e a autenticação ficam completamente comprometidas.

3. Propostas de solução/ aprimoramento da segurança

Alguns modelos propõem técnicas para acréscimo de segurança nas redes sem fio. Estes modelos estão atualmente fase de análise, sendo os que possuem maior destaque:

- utilização de mecanismos de proteção nas camadas superiores – uma solução para a maioria dos problemas nas redes sem fio seria a adoção de redes privativas virtuais VPNs (*Virtual Private Networks*). Existem alguns aspectos que devem ser considerados neste tipo de comunicação, principalmente sobre a degradação do desempenho da rede no estabelecimento de um grande número de conexões com um *gateway* VPN, além da perda de desempenho, consumo de baterias e processamento na adoção desta forma de comunicação em PDAs.
- utilização do padrão IEEE 802.1x para autenticação de dispositivos – propõe a utilização de variações do protocolo EAP (*Extensible Authentication Protocol*) para realizar a autenticação dos dispositivos [8]. Alguns estudos neste modelo apresentam problemas em relação a ataques do tipo *man-in-the-middle*, necessitando da criação de autoridades certificadoras (CAs) para as chaves trocadas entre os dispositivos, além da posisbilidade de sequestro de seção (hijack) [9].

Existem outras soluções sendo propostas por fabricantes de equipamentos, mas nenhuma delas foi padronizada, ou é amplamente adotada na prática. Salienta-se o protocolo WPA (*Wi-Fi Protected Access*) que está atualmente em estudos, e já se encontra em alguns equipamentos comerciais (apesar de não ser padronizado).

4. Linhas de Pesquisa Sugeridas

Tendo em vista as fragilidades do protocolo atualmente utilizado para garantir a proteção das redes sem fio, e dos problemas envolvendo as propostas de solução, torna-se evidente a necessidade de novas pesquisas em mecanismos de proteção nestas redes.

Estas novas pesquisas devem possuir como objetivo a construção de alternativas que incrementem os aspectos de segurança das redes, além de apresentarem condições de utilização considerando o impacto no desempenho das redes e a possibilidade de uso de dispositivos móveis com baixo poder de processamento e que utilizem baterias (PDAs).

Cria-se então, a necessidade de linhas de pesquisa integradas no aprimoramento de segurança com garantia de usabilidade real.

4.1 Pesquisa em protocolos segurança de redes sem fio

Para a adição de segurança de redes sem fio, sugere-se a criação de protocolos alternativos ao WEP, considerando as características particulares do tipo de comunicação sem fio. Deve-se dar atenção ao fato da forma de segurança estar

localizada no nível de enlace e na flexibilidade necessária ao novo protocolo para utilização em uma grande quantidade heterogênea de equipamentos.

A pesquisa deve estar centrada na criação de metodologias de testes e verificações das alternativas propostas tentando abranger o maior número de situações de ataque. É sugerida a adoção de verificação formal dos protocolos propostos.

Os novos protocolos de criptografia podem ser desenvolvidos através da alteração do código fonte dos *drivers* de placas de rede sem fio. Caso deseje-se apenas uma validação do mecanismo de criptografia, é necessária apenas a configuração de um ambiente *ad-hoc*. Nesse ambiente é possível a criação de uma arquitetura formada por equipamentos que trocam informações cifradas.

A adoção de mecanismos de segurança mais complexos cria reflexos evidentes no desempenho da rede. Especialmente tratando-se de algoritmos de cifragem de dados no nível de enlace que envolvem a sua adoção em equipamentos com baixo poder de processamento e necessidades especiais de economia de energia.

Deve-se, para verificar se os protocolos propostos contemplam estas necessidades especiais, realizar a criação de modelos das redes sem fio contendo os diversos tipos de equipamentos implementando as propostas. Sugere-se, então, que estes modelos sejam submetidos a testes em simuladores, com o objetivo de verificar o impacto das propostas no desempenho da rede.

4.2 Adição de mecanismos de autenticação e gerência de segurança

Outra alternativa para aumentar as características de segurança em uma rede sem fios, é a construção de um AP contendo mecanismos de segurança atualmente disponíveis.

Existem *drivers* alternativos capazes de fazer com que um computador coloque uma placa de rede sem fio em modo *máster*, capaz de assumir as funcionalidades de um AP. Isto possibilita adição de funções de autenticação, gerência e filtros de pacotes. Ao adicionar estes mecanismos, é possível aumentar a segurança de uma rede baseada em AP.

Alguns mecanismos possíveis:

- filtros de pacotes: pode-se adicionar filtros de pacotes para controle do tráfego entre a rede sem fios e a rede com fios, ou entre os dispositivos sem fio;
- mecanismo de identificação de intrusão: mecanismos de IDS (*Intrusion Detection Systems*) são *softwares* capazes de realizar uma análise do tráfego da rede, em busca de alterações do comportamento considerado normal (configurado pelo administrador) ou de assinaturas de ataques conhecidos. Esses mecanismos são uma ferramenta de grande importância para a gerência de segurança de redes atualmente;
- VPN: é possível a adição de túneis VPN entre APs ou entre um AP e seus clientes.

Deve-se salientar que os APs são dispositivos que operam em *layer* 2, ou seja, os mecanismos de segurança que operam nos níveis superiores estão sujeitos à configuração do AP para que possa ser feita a filtragem e análise do tráfego.

Os mecanismos de autenticação e criptografia propostos podem ser adicionados também nesse dispositivo, graças à flexibilidade de configuração de um AP em um computador.

5. Conclusões

Atualmente, os mecanismos de segurança disponíveis para redes sem fio apresentam-se ineficazes para cumprir suas funções. O mecanismo de confidencialidade utilizado pelo WEP não é seguro e pode ser comprometido através da utilização de *softwares* de análise estatística de tráfego. Com isso, tanto a confidencialidade quanto a autenticidade não são garantidas.

A necessidade de busca de alternativas passa por dois processos: alteração do WEP; e/ou adição dos mecanismos hoje disponíveis para segurança de redes. A validação de novos mecanismos de criptografia é um processo que deve ser realizado através de simulações e testes que garantam tanto a confidencialidade, quanto a praticidade dos novos modelos.

Atualmente, os autores deste trabalho realizam testes com mecanismos adicionais em APs, em busca da adição de segurança em redes sem fio.

Bibliografia

[1] IEEE 802.11. Part 11: **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. Disponível por www em: http://standards.ieee.org/getieee802/802.11.htm. 1999.

[2] ARBAUGHT, William A; et al. **Your 802.11 Wireless Network has No Clothes**. Department of Computer Science - University of Maryland. Disponível por www em: http://www.cs.umd.edu/~waa/wireless.pdf

[3] WALKER, Jesse R. **Unsafe at any key size; An analysis of the WEP encapsulation**. Intel Corporation, Oregon, 2000. Disponível por www em: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

[4] SCHNEIER, Bruce. **Applied Cryptography. Second Edition: protocols, algorithms, and source code in C**. John Wiley & Sons Inc. 1996.

[5] BORISOV, Nikita; et al. **Security of the WEP algorithm**. Disponível por www em: http://www.isaac.cs.berkeley.edu/ isaac/wep-faq.html

[6] FLUHRER, Scott; et al. **Weaknesses in the Key Scheduling Algorithm of RC4**. Cisco Systems Inc. Disponível por www em: http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

[7] **AIRSNORT**. Disponível por www em: http://airsnort.shmoo.com/

[8] RSA Security. **Improving Wireless LAN Authentication – A Description of the Authentication in 802.1x Standard**. RSA Security Inc. Disponível por www em: http://www.rsasecurity.com/go/slides2001Q4/wirelesslive/WirelessLANAuthentication2.pdf

[9] MISHRA, Arunesh; Arbaugh, William. **An Initial Security Analysis of the IEEE 802.1X Standard**. University of Maryland. Disponível por www em: http://www.cs.umd.edu/~waa/1x.pdf